FIG. 1

PORTABLE
DEVICE 15

MCU 25

RAM   25A

SYSTEM MEMORY 27

SYSTEM BUS 23

DSP 31

RAM

31A

ROM 32

HW CARD IF 29

MEMORY CARD 13

FIG. 2

requests for content and
keys received

encrypted content and
encrytped keys to decrypt
content transmitted

DEVICE
INTERFACE 39
ELECTRICAL
CONTACTS

13a. APPLICATION LAYER

communicates with device
accessing content

13b. SECURITY LAYER

controls access to logical
and physical layers

MEMORY CARD 13

13c LOGIGAL LAYER

files, tracks, directory
structure of content
corresponding to clusters,
AND encrypted keys

13d PHYSICAL LAYER

clusters of memory cells
33 with encrypted content
and keys

FIGURE 3A

13c. LOGIGAL LAYER

39

13d. PHYSICAL LAYER

33

| MEDIA IDENTIFIER |
| MEDIA KEY BLOCKS |

SYSTEM AREA 43

| MEDIA UNIQUE KEYS |
| RANDOM NUMBER KEY |

HIDDEN AREA 45

| ENCRYPTED TITLE KEY |
| ENCRYPTED CCI |

PROTECTED AREA 47

| ENCRYPTED CONTENT |

USER DATA AREA 41

39 ◄─► 35 CONTROLLER ◄─► 37

FIGURE 3B

TRACK (TKI) 300	→	AOB 304
	→	AOB 308
TRACK (TKI) 302	→	AOB 306
	→	AOB xxx
TRACK xxx	→	POB xxx

AOB 304

312 — AOB BLOCKS | ... |

316 — 318

320 — 318

FIG. 3C

|←——————————— 64 kbytes ————————————→|

| 1 | 2 | 3 | 4 | ...CHUNK 128 | |

49 "MKB" IMAGE

▼ 51   53   55   ▼

| 1 BYTE | 3 BYTES | | MULTIPLE OF 4 BYTES | |

RECORD   RECORD   RECORD KEY
TYPE   LENGTH

50 "MKB" CHUNK

|←——————————— 512 bytes ————————————→|

FIG. 4

DEVICE KEYS
$K_{d1}, K_{d2} \cdots$
(From Utilization Device)

MEDIA KEY BLOCK (MKB)
(Read From Card)

DECRYPT
MKB
(one Record at a Time)

~57

MEDIA KEY (K_M)

MEDIA IDENTIFIER (ID_{Media})
(Read From Card)

C2_G
FUNCTION

~59

MEDIA UNIQUE KEY (K_{mu})

FIG. 5

FIG. 6

FIG. 7

DECRYPTED CONTENT
OUT

CALLS/COMMANDS IN

SW 100 IN DEVICE 15

ENCRYPTED
CONTENT

SD CARD 13

FIG 8A

AUDIO INTERFACE 105

VIDEO INTERFACE 110

IMAGING INTERFACE 115

API 130A

COMMAND DISPATCHER 130

SD AUDIO ENGINE 140

SAPI
140A

NSAPI
140B

SD VIDEO ENGINE 150

SAPI
150A

NSAPI
150B

SD IMAGE ENGINE 160

SAPI
160A

NSAPI
160B

SSM MANAGER 180

NON SECURE FILE INTERFACE
170

SD SECURITY ENGINE 175

NSDD   SDD

190B   DEVICE DRIVER 190   190A

SW 100 IN
PORTABLE
DEVICE 15

SD CARD 13

DEVICE
INTERFACE
39

FIGURE 8B

RELATED API MODULES/CALLS
IN SW100 CODE

POWER UP
SYSTEM ⟋ 803

PRE-PLAY PROCESS ⟋ 805

805 10

POWER UP INITIALIZATION

805A
Initialize audio system (device 15)

- Get drive number
- initialize SSM 180, SDSE 175
- Initialize directory and file information (Playlist
and Track Manager) in media

SdInitAudioSystem

805B
Initialize/mount media
- MKB process
- copy media info 850 from storage device 13 into
memory of device

SdMountAudio

805.20

AUDIO CONTENT INTIALIZATION

805C-805L *(SEE FIG 8D)*

PLAYLIST AND TRACK INFORMATION
(POINTING TO LOCATION OF MEMORY CELLS
OF CARD 13 CONTAINING THE ENCRYPTED
CONTENT) COPIED FROM CARD 13 INTO A
RAM OF DEVICE 15

SdOpenTrack
SdGetPlayListCount
SdGetPlayList
SdGetTrackInfo

810

PLAY PROCESS

810A
SW 100 receives api calls (commands) that access
playlist info 860, track info 870, track index info 875,
and track general info 880 from ram of device 15

810B
SW 100 decrypts and decodes content from card
13 by accessing track general info 880 from ram of
device 15

SdPlayTrack
SdNextTrack
SdStopPlay
SdPauseTrack
SdResumeTrack
SdResetPlayList
SdForward
SdAddTKItoPLM
SdDelTKItoPLM
SdDelTKItoTMG
SdConvertMP3ToSA1
SdConvertAACToSA1

FIG 8C

POWER UP INITIALIZATION 805 10
(See Fig 8C)

805C
User interface of device 15 calls
SdGetPlayListCount

805D
SdGetPlayListCount refers to Media
info block 850(drivenum etc..) and
returns the number of playlists
available in card 13

805E
User interface of device 15 calls
SdGetPlaylist

805F
SdGetPlaylist refers to Media info
block 850 and copies values from card
13 into playlist info block 860 in
memory of device 15 for access by
device 15 user interface

805G
User interface of device 15 calls
SdGetTrackInfo

805H
SdGetrackInfo refers to Media info
block 850(drivenum etc..) and playlist
info block 860 and copies values for
each track from card 13 into track info
block 870 in memory of device 15 for
access by device 15 user interface

805I
User interface of device 15 calls
SdOpenTrack

805J
SdOpenTrack refers to Media info
block 850, playlist info block 860, and
track info block 870 and copies some
(plisttime, plistnum, tracknum,
firstAOB, currentAOB) values for
current track from card 13 into Track
General Info block 880 in memory of
device 15 for access by device 15 user
interface

805K
SdOpenTrack refers to media info
block 850 and playlist info block 860
and copies values for track indiex info
from card 13 into track index info block
875 into memory of device 15

805L
SdOpenTrack refers to Media info
block 850 and playlist info block 860
and copies remaining values for
current track from card 13 into Track
General Info block 880 in memory of
device 15 for access by device 15
user interface

PLAY PROCESS 810
(See Fig 8C)

FIGURE 8D

AUDIO CONTENT
INITIALIZATION
PROCESS 805.20

Track Gen Info
SanDisk
cmd
audioformat
sampfreq
appAttrib
sizeAOB
currentAOB
firstAOB
lastAOB
countAOB
syncword
seekposAOB
trkElapsedTime
trackTime
bytesize
elementplaytime
tracknum
fwTime
fwNext
tracksInPlist
pListTime
elementsize
elementoffset
currentelement
totalelements
plistnum
fdAOB

880

Media Info
pTGInfo
SanDisk
drivenum
security
mounted

850

Track Info
trackTime
bytesize
tkisInTrack
tracknum
index
trkInformation[...]

870

875

Track Index Info
trackTime
seekpos
bytesize
aobsize
audio_attribute
app_attrib
tkicount
lastTKI
elementplaytime

860

Playlist Info
pListTime
tracksInPlist
index
Length
pListName[...]

PRE-PLAY STRUCTURES
FIG 8E

CORRESPONDING API
IN CODE

SEC_AKE API

SEC_ENC_TKEY API

SEC_DEC_TKEY API

SEC_GETCCI API

SEC_UPDATECCI API

PROCESS MKB IMAGE

MKB -> Km -> Kmu

— 205

PARTIALLY
PROCESS AKE

Kmu -> Ks

— 210

DELETE Kmu — 213

USE SESION KEY (Ks) TO
DECRYPT DOUBLY
ENCRYPTED TITLE KEY

E(E(Kt)) -> E(Kt)

— 215

STORE E(Kt) IN A
MEMORY OF THE
DEVICE — 220

READ PORTION OF TRACK — 225

CALCULATE Kmu — 225a

DECRYPT E(Kt)

E(Kt) -> Kt

— 225b

USE Kt TO
DECRYPT
CONTENT OF
BUFFER — 225c

DELETE Kt — 225d

DELETE Kmu — 225e

ALL PORTIONS OF
TRACK READ? — 230

NO

Y

NEXT TRACK — 235

FIGURE 9

SET THE BUFFER POINTER TO THE DATA BUFFER AND CLEAR THE BUFFER OFFSET — 205.5

IS CN EQUAL OR LARGER THAN 128 — 205.10

ERROR — 205 15

INCREMENT CN AND LOAD NEW DATA INTO BUFFER — 205.20

— 205

UPDATE THE BUFFER OFFSET — 205.25

SET THE BUFFER POINTER TO THE BUFFER OFFSET — 205.30

— 205 40

205.42

READ BUFFER AND CHECK RECORD TYPE FOR EACH CHUNK 1-128

N

CMKR?

205 44 — VMKR?

205.46 — CCMKR?

205 48 — EMKR?

N

N

N

205 49

UPDATE AND SET THE BUFFER POINTER AT A NEW OFFSET

205 49 — UPDATE AND SET THE BUFFER POINTER AT A NEW OFFSET

UPDATE AND SET THE BUFFER POINTER AT A NEW OFFSET

205.49 — UPDATE AND SET THE BUFFER POINTER AT A NEW OFFSET

USE Kd FROM DEVICE 15 TO CALCULATE Km

IS CALCULATED Km SAME AS STORED Km?

USE Kd FROM DEVICE 15 TO CONDITIONALLY CALCULATE Km

IS Km VALID AT THE END OF RECORD? — 205.70

205.50

RETURN PASS (DEADBEEF)

205.75 — RETURN FINAL Km

205.55

205 60

205.65

GOTO STEP 210 OF FIG 9 — 205.85

REJECT MEDIA — 205 80

FIGURE 10